BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AFMC INSTRUCTION 33-501

21 JUNE 2004

Communications and Information

ONE AIR FORCE--ONE NETWORK

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFMC/ITXI (Mr. Ron Jones)
Supersedes AFMCI 33-501, 31 October 2003

Certified by: HQ AFMC/ITX (Mr. Gary Brooks)
Pages: 8
Distribution: F

This instruction implements AFMCPD 33-5, *One Air Force--One Network*. It explains the specific policy and procedures for the information infrastructure projects supporting the achievement of the One Air Force--One Network concept. This instruction does not apply to U.S. Air Force Reserve or Air National Guard units or members.

SUMMARY OF REVISIONS

This AFMCI supersedes AFMCI 33-501, 31 October 2003. A bar (|) indicates revision from the previous edition.

1. Information Transport projects.

1.1. Combat Information Transport System (CITS)/Network Operation and Information Assurance (NO/IA). CITS NO/IA, a part of the CITS program, is an Air Force downward-directed program. The NO/IA provides the design, acquisition, implementation, and upgrade of the boundary layer infrastructure, network management, and information protection tools/capabilities for the 129 CITS-supported installations and ten regional Network Operations and Security Centers (NOSCs) worldwide. AFMC installations must ensure the CITS NO/IA-provided architecture, configuration, and products are implemented and utilized as designed. Any non-compliant architecture or configuration must be approved by MAJCOM and CITS Program Management Office via waiver prior to implementation, or it will be realigned to the standard configuration by the installation team during future upgrading/installation. To request a waiver, the installation submits a waiver request using the CITS-provided template to the MAJCOM CITS/NO/IA office for review and coordination. If MAJCOM concurs on the request, MAJCOM will forward the waiver to the CITS Configuration Control Board at AFCA, the CITS lead command office, for AF-level approval.

1.2. The CITS Program Office is implementing the One Air Force--One Network concept. AFMC fully supports the MAJCOM-centric solution. Currently, Air Force is further proposing an AF region-

alization solution. Under the regionalization solution, the ten NOSCs would be integrated into four NOSCs and would be known as the Integrated NOSC (INOSC). This proposed design may effect many of the functions now performed by the NOSC under the MAJCOM-centric direction. In alignment with AF MAJCOM-centric direction, the AFMC NOSC is performing the following functions for the base Network Control Centers (NCC) which started in calendar year 2002. This effort had no impact on the base resources in calendar year 2002, but should provide near real-time network-status reporting to AFMC/CC; reduced troubleshooting time; more proactive fix actions by watching for events/anomalies that threaten/impact network performance or jeopardize network security, improved compliance with AF standard configurations, and reduced vulnerabilities by providing synchronized security updates (Time Compliance Network Orders, {(TCNO) Notice to Airmen, etc.} to e-mail servers, centralized public web servers, and timely external ISS scans for AFMC bases. For detailed information on all aspects of our NO/IA efforts, please visit **https://www.afmc-mil.wpafb.af.mil/organizations/HQ-AFMC/SC/scp/scpc/cits/index.htm**

1.2.1. CITS NO/IA tools provide capabilities for remote monitoring and management of a base's boundary and network devices management and protection. Currently, we only take advantage of their monitoring capability. Eventually we plan to extend to management capability.

1.2.2. Remote management of base's consolidated e-mail servers.

1.2.3. Conduct vulnerability scans of all devices. Provide the base Information Assurance office the results for fix action or Designed Approval Authority (DAA) acceptance of the vulnerabilities.

1.2.4. Provide centralized management of static public web service.

1.2.5. Provide automated ticket escalation from the base NCCs to the NOSC.

1.2.6. Provide event management, notification, and reporting of the AFMC enterprise network.

1.2.7. Develop plan for future remote management of each base's firewalls.

1.3. Enterprise System Management (ESM). ESM is a collection of people, tools, and processes that provides the capability to manage the entire AFMC Enterprise Network from a single management framework. The first spiral of ESM, called Spiral 1A or Desktop Management (DTM), provides for the management of computer desktops and servers attached to the AFMC unclassified network from a single console. DTM will provide the following capabilities: remote control, hardware and software inventory and distribution of software. Tivoli is the selected tool to provide this capability. Spiral 1B provides the first truly enterprise systems management capability to AFMC by providing a tiered system with network device event, fault, and performance management from a single integrated management environment.

1.3.1. ESM will enable the command to provide real-time Time Compliance Network Order response and verification. Therefore, it is mandatory that all tenants using the same network backbone at an AFMC site use Tivoli, as managed by the site communications unit. When all tenants attached to each site's network infrastructure are operational, Final Operating Capability (FOC) will be achieved. All deploying site communications units will follow the Tivoli-provided architecture and maintained configuration currently managed by the ESM Program Management Office (MSG/MM) and eventually the AFMC NOSC, when transitioned to the sustainment phase.

1.3.2. No AFMC funds are to be expended acquiring or maintaining other tools with similar capability outside the AFMC ESM and AF CITS Network Operations/Information Assurance (NO/IA) projects.

1.4. Voice over Internet Protocol (VoIP). Modest investments, $100K or less, in VoIP are appropriate for exploring future potential, but widespread use of VoIP technology is discouraged until further business and operational issues can be resolved. Requirements for new VoIP test projects, as well as any existing VoIP projects, must be identified and forwarded to HQ AFMC/ITX for review and coordination. Include project description, requirements, and implementation plan. We will then forward the project to AFCA/GCLV for coordination and approval.

2. Information Computing Projects.

2.1. Regionalization. Regionalization builds on the work done over the past five years to consolidate and standardize our computer network operations. On a base-centric level we have been centralizing network management, consolidating our core servers (file, print, web), while at the MAJCOM level implementing AFMC enterprise storage solutions, and standardizing business application operating systems. This work has made AFMC's IT perform more efficiently and improved network defenses by allowing IT professionals to close "backdoors," survey the cyber-boundaries, and perform more sophisticated and granular security management. Our chronic resource shortfalls represent our greatest vulnerability—too few staff, insufficient funding to support local redundancy. Regionalization uses state-of-the-art technology to overcome these limitations.

2.1.1. Regionalization is the further consolidation of business applications and network management into geographic areas—a single "hub" supporting multiple AFMC bases, holding the business data accessed by web-enabled applications. Regional control staffs will employ remote management tools to more efficiently oversee network operations. Most importantly, redundancy will be built into the systems, with failover capability between regions. This will ensure continuity of operations and disaster recovery that provides quick restart of network services. AFMC customers and operators will have an IT architecture capable of supporting enterprise business regardless of man-made or natural interference with a segment of the system.

2.2. Directory Services. We have obtained interim authority to build and operate the AFMC Business Continuance/Concept of Operations (BC/COOP) Architecture and Advanced Messaging system. Interim authority is also granted to employ Microsoft's Exchange 2003, Live Communications Service 2003, Windows 2003 Enterprise Edition, and Microsoft Digital Rights Management Server 2003. Our current minimum desktop operating system for all AFMC user computers is Windows 2000; however, AFMC has initiated a migration to Windows XP for desktop users.

2.2.1. HQ AFMC is now deploying a BC/COOP and advanced messaging infrastructure that will bring greatly enhance storage and messaging capabilities to the enterprise, but to fully utilize all the capabilities this technology brings requires that all AFMC user computers operating systems be upgraded to a minimum of Microsoft Windows XP and that all AFMC domain controllers be upgraded from Windows 2000 Server or Advanced Server to Windows 2003 Server or Advanced Server. Therefore, full deployment of the Windows XP operating system on all AFMC desktop computers within the enterprise is authorized. In addition, AFMC desktop computers will be upgraded from Microsoft Office 2000 to Office 2003 to provide users the best, most seamless transition experience from our current e-mail systems (DMS Exchange 5.5) to Microsoft Exchange 2003. This upgrade gives AFMC the best opportunity to leverage its investment in the Microsoft Enterprise Agreement. Therefore, interim authority is granted to deploy, install and configure Microsoft Office 2003 on AFMC user desktop systems through 18 Dec 04, or until such time as the IAC and HQ AF-CIO grant formal approval for use of Office 2003 on AF networks. Once the

BC/COOP infrastructure is in place, AFMC will conduct full system testing to complete the certification of the BC/COOP and to obtain a Certificate to Operate (CTO).

3. Information Assurance Projects.

3.1. Public Key Infrastructure (PKI). PKI is part of the DoD's key management infrastructure, which is a critical piece of the DoD's information assurance program. PKI refers to the framework and services that provide for the management of public keys and certificates. These keys and certificates are used to protect data transmission (data integrity and confidentiality) and confirm the identity of participants (authentication and non-repudiation). The DoD Chief Information Officer (CIO), in a series of memoranda, has mandated the following actions.

3.1.1. All private DoD and DoD-interest web servers must use DoD PKI server certificates to enable the web server's Secure Sockets Layer (SSL) for server authentication and to limit access to that web server. The suspense for this action was Dec 00. AFMC is in compliance with this mandate.

3.1.2. All eligible DoD personnel and contractors will eventually be issued Class 3 PKI certificates. These certificates will be issued on the Common Access Card (CAC). As of 20 Apr 04, approximately 90% of eligible personnel in AFMC already have a CAC. AFMC is considered in compliance with this mandate.

3.1.3. Some e-mail sent within the DoD will be digitally signed using Class 3 PKI certificates. AFMC published a set of PKI business rules to assist e-mail senders in determining which messages should include digital signatures. See the published AFMC PKI business rules at **https://www.afmc-mil.wpafb.af.mil/HQ-AFMC/SC/scp/projects/pki-business-rules-afmc.doc.**

3.1.4. All private DoD and DoD-interest web servers will perform client authentication using Class 3 PKI certificates. This allows the private web servers to positively identify those connecting to that server.

3.1.4.1. Private web servers are those that contain information not releasable to the general public or is intended only for a subset of the entire DoD or AF. An example of the former would be a base's home page accessible by anyone in the .mil or .gov domain. An example of the latter is the web-enabled base phone directory available only to people on that base.

3.1.4.2. HQ AFMC/IT directed that web content must be migrated onto the AF Portal and the physical web servers be shut down or re-utilized. Doing so will satisfy the DoD CIO mandate because the AF Portal will perform client authentication before access is granted.

3.1.4.3. Webserver administrators who are not able to comply with this mandate must submit a formal waiver request. The waiver request format and process may be found at **https://www.afmc-mil.wpafb.af.mil/HQ-AFMC/SC/scp/projects/pki-happenings.htm#pke_waiver**.

3.1.5. All DoD unclassified networks shall be enabled for hardware token, certificate-based access control. Currently, this hardware token is the Common Access Card. AFMC is in the process of enabling its networks to satisfy this mandate.

3.1.6. Any person, application, or system that requires support from a PKI must use the DoD PKI unless explicit approval is granted by the DoD PKI Program Management Office.

3.1.6.1. This applies, but is not limited to user, device, code-signing and server certificates.

3.1.6.2. This does not apply to the Defense Message System High Grade Service which uses its own PKI to generate FORTEZZA cards.

3.1.7. Persons to whom DoD PKI certificates are issued must protect those PKI certificates and their associated personal identification numbers (PIN) IAW the DoD PKI Certificate Policy and AF System Security Instruction 3034, FORTEZZA User Requirements (FOUO). Appropriate protection must also be afforded the token (e.g., the CAC or a floppy disk) on which the DoD PKI certificates are stored.

3.1.8. USAF and USAF-contracted developers of applications and systems intended for the AF must consider use of PKI certificates if the application or system requires identification and authentication of its users. The DoD as a whole is moving away from the traditional user ID and password and towards two-factor authentication made possible by PKI certificates and PINs.

3.1.9. Organizations purchasing Public-Key enabled commercial-off-the-shelf products must ensure that these products are compatible with the DoD PKI, the tokens on which the PKI certificates are stored (CAC, floppy disk, universal serial bus plugs, etc.) and the hardware/software used to access the PKI certificates.

3.1.10. The AFMC public key infrastructure, which uses a Microsoft certification authority, will issue only device certificates. No user certificates will be issued from the AFMC PKI. All user certificates will be issued from the DoD PKI.

3.1.11. AFMC bases and sites will employ CAC PIN Reset (CPR) workstations as the primary resource for "unlocking" the CAC's integrated circuit chip. As much as possible, persons at AFMC bases and sites should not visit the base Military Personnel Flight if only to reset a CAC's PIN.

3.1.11.1. Each AFMC base or site will appoint a primary and alternate Trusted Agent Security Manager (TASM) who will oversee operation of all CPRs at that base or site.

3.1.11.2. Each AFMC base or site may also have CPR Trusted Agents (CTA) who are the operators of the CPR workstation. Each base or site will decide for itself—within the constraints of DoD, AF, and Defense Manpower Data Center (DMDC) rules—who may serve as CTAs and the total number of CTAs at that base or site.

3.1.11.3. The organization where the CPR workstation is installed is responsible for its proper operation and maintenance, in accordance with DoD, AF, and DMDC rules. Sustainment (e.g., tech refresh) of the workstation is also the responsibility of that organization.

4. Information Management Projects.

4.1. AF Portal. The AF selected BroadVision as the enterprise portal product and is integrating the portal with the Global Combat Support System-Air Force (GCSS-AF) integration framework. AFMC fully supports the AF solution and the AF vision. One Air Force--One Network--One Portal. AFMC is leveraging the AF investment by using BroadVision as the command content management product fully integrated with the AF enterprise portal solution.

4.1.1. The AF Portal will be the personal one-stop shop for on-line information and resources tailored to individual customer needs. Unlike other web sites containing an avalanche of useless

information, the AF Portal will offer a relevant flow of information based on an individual customer's profile (job and interests), improving their day-to-day capability to perform their duties. The AF Portal will establish standard web views with a consistent look and feel; implement a powerful content management capability which will allow automation of coordination, publication, and expiration functions for current and relevant web content; and provide a common platform for all AF web initiatives. HQ AFMC plans to migrate all static web content across AFMC to the AF Portal and register all AFMC members (military/civilian/contractor) on the AF Portal by Jan 04.

4.2. Lifecycle of Information Software Solutions (LISS).

4.2.1. AFMC has embraced e-Business as a strategy to increase workforce productivity and facilitate decision-making. To support implementation of e-Business, the AFMC CIO Council formulated a set of life-cycle information management requirements **https://www.afmc-mil.wpafb.af.mil/HQ-AFMC/SC/scp/projects/liss.htm#Documents**. These requirements include electronic records management, document management, collaboration, and workflow automation. We have developed a business case that shows a positive return on investment by implementing an automated system for Information Management.

4.2.2. The AF-CIO is sponsoring an effort to identify an AF standard Enterprise Information Management (EIM) solution. AFMC will conform and align with the AF EIM standard once standards or a standard tool is identified.

4.2.2.1. The AF-CIO has identified two tools as part of the EIM solution, which AFMC supports as standard tools. These include PureEdge for forms design and usage, and AF Knowledge Now for collaboration via Communities of Practice (COP).

4.2.3. Organizations that have already invested in EIM solutions (e.g., Livelink, Documentum) may continue their efforts until the rest of the AF standard is identified and a transition plan developed.

4.2.4. For any organizations procuring any new document or records management and workflow EIM solutions, Livelink is the AFMC standard. By procuring the AFMC standard, migration to the eventual AF standard will be easier as there will only be one migration path.

5. e-Business. Our goal is to provide a process-centric enterprise. Leveraging e-Business capabilities and technology will increase efficiency, speed and effectiveness of all AFMC processes. This will facilitate efficient weapon system acquisition, reduce software development and maintenance costs, and provide the warfighter access to more abundant and timely information. The AF Portal will be the single-service delivery point for all IT products and services.

6. Information Enterprise Projects.

6.1. AFWay System. The Information Technology Management Reform Act (ITMRA) of 1996 provided the impetus to significantly improve the way AF acquires and manages IT. The mandate to lower the total cost of ownership and gain control of IT tracking led to the development of the AFWay system, which is on-line at **https://afway.af.mil.** AFWay has been designed to reduce customer workload and to provide the AF-CIO visibility into hardware and software purchases for the IT enterprise. Additionally, AFWay allows for necessary variations to accommodate unique MAJCOM requirements and processes while maintaining AF-CIO standards.

6.1.1. As a result of system updates provided in version release 2.4, which addressed the customizable workflow requirement identified by the AFMC Functional Review Board (FRB) as a MUST HAVE, AFMC is now enforcing the mandatory usage policy for the acquisition of desktop/laptop computers throughout the command. Furthermore, to ensure pre-negotiated contract holders receive a fair opportunity, competition requirements for individual orders shall be adhered to when soliciting quotes estimated to exceed the micro-purchase threshold. Contracting Officers shall solicit, at a minimum, those contract holders in the specific category of products being acquired. Contracting Officers are required to award orders to contractors that can provide products that represent the best value to the government, and they shall follow the ordering procedures at FAR 8.404(b)(2) when determining best value.

6.2. AFMC Standard Desktop Configuration. Effective immediately, AFMC will comply with standard mainstream buying configurations as identified in the Infostructure Technology Reference Model (iTRM) and will use the Air Force Information Technology Commodity Council's (AF ITCC) quarterly enterprise buying process via AFWay (**https://afway.af.mil**) for all desktop and laptop computer purchases. In conjunction with this process, the AFMC CIO has established the following technology refresh policy: desktop computers should be replaced no sooner than every four years; laptop computers should be replaced no sooner than every three years; monitors should be replaced no sooner than every six years; and printers should be replaced no sooner than every five years. Requirements for desktops and laptops that fall outside the mainstream configurations, or planned purchases not using small business or the enterprise buy process, must be approved by appropriate MAJCOM or Air Staff functional CIO. This waiver authority will not be delegated. A copy of all waivers must be forwarded to AF-CIO/R. The iTRM can be accessed at the following web site: **https://itrm.hq.af.mil**. In addition, AFMC has entered into a five-year software Enterprise Agreement with Microsoft. The AFMC Enterprise Agreement allows the latest version of the following Microsoft products on one computer during the term of the agreement: a) Office Professional; b) Windows Desktop Operating System (OS); and c) Core Client Access License. AF-CIO Policy Memorandum 03-05, 8 May 03, Desktop Operating System Upgrade to Windows XP, establishes Windows XP Professional, configured to meet minimum security benchmarks as identified by the Enterprise Network Operations Support Cell, as the Air Force standard desktop computer operating system and establishes 31 Mar 06 as the sundown date for Windows 2000. Refer to **https://www.afmc-mil.wpafb.af.mil/HQ-AFMC/SC/sca/policy/guidance.htm** for the latest AFMC Desktop Configuration Standards.

6.2.1. AFMC Home Use Program (HUP). AFMC has established an Enterprise Agreement (EA) with one of the DoD-Enterprise Software Initiative providers to acquire Microsoft licenses and products AFMC-wide. As a result of this EA, AFMC has acquired "Home Use Rights" for all AFMC employees (AFMC military, civil service, and contractors which are being provided government computer equipment and a government (af.mil) e-mail address). "Home Use Rights" give AFMC employees the right to install the same Microsoft Office desktop application programs on their home computer as they use on their office computer (including Office Pro, Project and Visio).

6.2.1.1. To access the Microsoft HUP web site, please follow these procedures: Go to **https://hup.microsoft.com/**. Select the country to which you wish your order to be shipped to and choose the language for viewing the order web site. Enter your corporate e-mail address (must end with af.mil) and insert the following program code: 927B23E0D7. This program code is assigned to AFMC for our sole use in accessing this site, and you must not share this

number with anyone outside our organization. Place your order on-line and it will be shipped to the location you have chosen. Please note that a fulfillment fee will be charged to cover packaging, shipping and handling costs. These procedures are the only means to be used in obtaining the Microsoft application programs for your home use.

KENNETH I. PERCELL, SES
Director, Information Technology